Agent Virus of Cooperation (Avicoop): an Intelligent Model of Cooperation and Collaboration Based on the MAS for Data Exchange in Ad hoc Network.

Thomas Djotio Ndié[1] and Claude Tangha[2]

[1] National Advanced School of Engineering, Department of Computer Engineering, University of Yaounde 1, LIRIMA/MASECNESS
Yaoundé, Center 00237, Cameroun

[2] National Advanced School of Engineering, Department of Computer Engineering, University of Yaounde 1, LIRIMA/ALOCO
Yaoundé, Center 00237, Cameroon

Abstract

We propose in this paper a response to the problem of cooperation and collaboration between nodes in a mobile ad hoc network (MANET) for intelligent data relays from one source to a destination. In their operation, each routing protocol relies on the support of each node for end-to-end messages routing by completely ignoring the autonomous nature of the node that is to be free to accept, reject, relay or otherwise simply manipulate the protocol's principle. This random and unpredictable behavior of the node impacts on the routing effectiveness in the global network. Our approach is based on multi-agent systems (MAS) and game theory, especially the iterated version of the Prisoner's Dilemma. The proposed model is validated by a prototype.

Keywords: *Avicoop, Cooperation, data exchange, Mobile Ad hoc networks (MANET), MAS, Game theory*

1. Introduction

A mobile ad hoc network (MANET) is a mesh network which consists of a collection of devices or nodes linked by wireless and/or mobile connections without the use of any pre-established infrastructure to perform the essential network functions as data routing or conveying [1], [2]. In such networks, each node has autonomy in terms of decision making. Therefore, each device acts on the benefit he derives from his act. This is the birth of strategic behavior within the network. Each node equally has its own energy supply, autonomy management, capacity storage management... Generally, equipments consist of on-board batteries. This power factor set with other requirements of the node leads to the adoption of opportunistic behavior designed to optimize the exploitation of these resources.

In general, each node has constrained and limited radio coverage. It is aware, thanks to various existing techniques (such as routing/switching tables, dynamic updating), of the presence and position of each device in the network but does not always have necessary performances for direct communication. It is then essential to be relaying messages through the network. This fact is universally accepted by all. This is one of the basic assumptions of the development of all ad hoc routing protocols [3], [4]. According to the mechanisms of road creation and maintenance during packet routing, author of [5] classifies routing protocols into two groups: first are proactive protocols (DSDV (Destination-Sequenced Distance Vector routing), FSR (Fisheye State Routing), etc) based on roads pre-establishment using the routing tables periodic updates and second, reactive protocols (DSR (Dynamic Source Routing) [3], AODV (Ad hoc On Demand Distance Vector) [4], etc) which seek roads when the need of packet routing arises. Each group asserted either by a contribution in terms of energy consumption optimization, path calculation performance or dynamic topology control.

At their origin, ad hoc networks were set up by a single organization to meet a specific need: help, various military operations, just to name a few. Here, nodes are all working to achieve a common goal. In practice, the tasks are clearly defined and a supervisor is available. In this case, the nodes do not have much choice but to perform the tasks they face. Today, an ad hoc network is a more elaborate, more sophisticated and durable system. Centralized and homogeneous systems become decentralized and heterogeneous domains and interaction involving several subsystems whose interests are not the same and therefore one may completely ignore the pursuit of others. Sometimes the interest may be completely contradictory (competitive situation). In this case, can we still assume the cooperation of nodes in the operation or functioning process and mechanisms of the setup network? Answering

yes to this question means that: in a social environment (shopping center, urban center, …) you can define the rules of the game and fully trust stakeholders for its implementation. It also means that in a company, an association or federation, we can give the rules of procedure and submit them to members who will unanimously respect them. There are always random and unpredictable behavior that impact on the overall behavior of the system.

Clearly, if decisions are made based on reason as is the case in an ad hoc network, unanimity is not acquired for the principles of operation of the network defined by a protocol. A concern emerges from this brief analysis: the implementation of an effective cooperation mechanism which makes the collaboration between the entities available in an ad hoc network. We propose in this paper to study and implement mechanisms that will promote adherence to the principles of the nodes of cooperation and collaboration. The rest of the article is organized as follows: the section 2 explores similar works which we refer to for various trends. In section 3, we present the Avicoop (Agent Virus of Cooperation) model. Before concluding and presenting future directions of research on the model, we discuss in sections 4 and 5 its implementation and analysis.

2. State of the art on the issue of cooperation in ad hoc environment

The studies undertaken by Abdesselem Beghriche et al in [6] show that different approaches setup to solve collaboration and cooperation problems all, almost share the same basic ideas that are to observe all network devices to identify and respond to failure events. What marks the difference between the approaches is more: (1) the definition and characterization of the equipment failure. (2) The policy of detection of nodes convinced of the failure. (3) The different ways of handling equipments based on their behavior.

Note that from one author to another, the harmfulness of equipment for the ad hoc routing service is defined in much the same way. A node that refuses willingly and deliberately to not relay the packet of the other shows a clear nuisance. It is the same for the one which floods a device or set of equipment with misleading messages in order to congest the network. Another type of disturbance is manifested by the violation of the integrity and confidentiality of messages [7]. We subscribe to these criteria for identifying nuisance and now consider as a hypothesis for our approach. That said, it is natural to ask how to detect nodes, all nodes and only nodes with one and / or another of these shortcomings. The answer to this question will locate any solution in one of three categories.

- The first category: They advocate the existence of a certification authority that will coordinate the inputs and outputs of the network, which also goes through a monitoring system to monitor the behavior of each device.
- The second category: Instead of a central authority, there is a local authority that controls it. The reconstruction of society is dynamic due to the mobility of the network. Each node to lead this operation is selected by a local mechanism that takes account of his service (Hierarchical models)
- The third category: The idea here is to completely decentralize operations, render completely local treatment that is at the level of each equipment. This offers a considerable gain in administrative operations. Our approach falls into this category (Flat models).

As part of his master thesis, Andriamady [8] made a literature survey on the issue and presented in details the controls and limitations. Control by the meter is to provide each node a counter that reflects the node's behavior either during its operations or during a test event Police carried out regularly at each node (for example, it is to send a certain number of test packets tests to the node and observe its behavior). In [9], Buttyan and Hubaux describe a protocol that controls each node. The nuglet counter is presented as a counter that is incremented at sending the message as a sender and which is decremented when relaying a message. Critics have found as the major drawback that the node which wants to send a packet paid in advance (the counter is decremented); so that if the message does not arrive its destination, then it is the loser. Such a system is also subject to many manipulations or attacks such as fraudulent attempts to increment the counter are one, but the authors say they have made a consistent design. This approach has been of interest except that we have also found a number of shortcomings:

- The criteria of the decision making is that the node can transmit over the network when its meter registers a positive number. This means that a node will send a number of posts equivalent to the number of messages relayed. In the case where the number of requirements for sending messages is not equivalent to the number of relayed packets, the node can be penalized. It may happen that depending on the type of service that it renders, based on its position on the network or based on other settings related to the operation of a node, that it can be legitimately forced to send more messages than it receives to relay. The Buttyan and Hubaux [9] solution penalizes such equipment.

- The same solution does not guarantee the confidentiality and integrity of the message. In that a node can alter a packet to be relayed without being punished.
- Malicious nodes remain in the network and are unknown of others. A node which decides to simply harm the network without having to send messages feels itself at ease because it constantly receives messages and simply destroys them, thus penalizing others though they enjoy a good reputation.

Control by reputation calculation intended to identify the equipment in suspicious behavior and inform the community. Marti, T. et al in [6] propose a model based on this technique. The decision of emitting here is provided by the results of observation of each node by his entourage. The result is then propagated through the network thus avoiding malicious nodes during the operation of sending messages. This approach is also subject to much criticism:

- Lack of formal specification for the type of motivation that the system guarantees.
- It is based on the broadcasting mechanism for each node to monitor the environment, which can be very expensive. Note also that the presence of asymmetric connections compromised the operation.
- Malware equipments can unite to relay their packets between them.

Our approach is a compromise between the two previous. It aims at making the intelligent decision-making process by implementing in each device an agent that has behavior enabling it to make right decisions at the right time. We call this Agent Virus of Cooperation (Avicoop).

3. Presentation of Avicoop model

The approach of virus agent of cooperation is mainly based on the social model of establishing the rules of life in a social group, to have them ratified by anyone wanting to belong to the group and then apply them to the functioning of the group. Here a node can be a computer, a mobile phone or compatible. We shall call indifferently in the following equipment or node to mean the same thing in the context of MANET [10], [11].

In practice, the social context for us is represented by all the equipments belonging to a MANET. The rule of life is that the equipments have a duty to relay if necessary packets passing through them. The facility that willingly fails in this task incurs a penalty proportionate to the seriousness of its failings. Therefore fixed, the ratification of the agreement by an equipment wanting to belong to the network is to receive the Avicoop application which is a policeman agent, constructed to monitor compliance with the agreement. One can add other specifications that reflect the reality of the network. For example, one may want in a heterogeneous network of mobile phones and computers, that certain types of messages to be routed from one computer to another, may, due to their size, not pass through phones. Thus, Avicoop must be informed to avoid penalizing a mobile phone that receives such a packet to be destroyed for lack of power because its initial opportunistic behavior is to optimize its energy resource. For a start, we consider a rough model which takes into account some specifications outlined below. Note however that this can be refined to better reflect the realities of the network.

Another challenge of routing, but not the least, is to ensure the confidentiality of message content. Message encryption is illustrated so far as the ideal solution to this problem. It almost always leads to a need for key exchange between the correspondents. This requires a large traffic flow in order to complicate the calculation of the code by an intermediate device that listens to the exchange. The Avicoop application embeds an encryption security model that bypasses traditional approaches to dissimulate the encryption key to others. We assume that each node that wants to send a message through the network, first submit its message to the Avicoop encryption module that encrypts the message before any mailing. Similarly, any equipment that receives the message knows nothing of its content; it is even Avicoop that must decrypt this content to make it understandable to the node. The full decryption of a message occurs only once the Avicoop module of the destination recipient acknowledges the message. For a routing need, the message is decrypted in part if necessary in transit stations.

3.1 Properties of Avicoop

1) Transmission Request Protocol (based on DSR[3]):

The application must be able to move completely to an agent at its request made by simple radio contact with an agent which has already been installed the program. This constraint is intended to facilitate the addition of a new element in the network. Each node has the ability to take delivery of another, thus avoiding the need for a certification center or centralized administration. An agent that wishes to join the network must, according to its geographical position, identify the nodes it can directly reach. It addresses its application (in the form of a standardized message) to the nearest and, after a delay, if it receives no response, it restates its request for another agent and so on. The first positive response received is

subject to an acknowledgment informing the sender of the adoption of its offer. This response will permit in a subsequent study to track each equipment upon its arrival in the network by mobile agents - based mechanism

In our model, we assume that each agent before any application for membership in the network has set up to accommodate the module. We simulate this home frame with a generic program that will accept the application and instantiate Avicoop itself modeled by a set of behaviors that agents must integrate.

2) Automatic administration.

The program must be autonomous in that it must be able to study the behavior of a host and make appropriate decisions without the intervention of the user's host. Beside that, a set of mobile agents will in turn move from one host to another for purposes of configuration and maintenance. They are launched with the application or during the lifetime of the network by a planner as needed.

3.2. Application operation

The activities are divided among several processing modules that coordinate.

1) Processing Module.

Within this module, each node that wants to send a packet to another must submit the packet to the module to encrypt the entire contents of the package. Each node that receives a packet does not know a priori the recipient of the packet. It must submit to its processing module that must decrypt the packet. During this process, when module that perfectly knows the host which accommodates it notes that the packet isn't intended for this host, it leaves the packet contents encrypted. However, the rest (header) of the packet is decrypted to allow the host manager to appreciate and make the right decision. In the case of a packet that only needs to be relayed, the node identifies the next destination and submits the packet to the module that reconstructs the encryption. During this process, the packet processing module raises statistical data that will enable it to assess the reputation of the node and take the appropriate decision.

2) The calculation module of reputation and punishment.

This module is responsible for conducting fact mainly statistics on the number of packets received and relayed, the number of received packets for the node in question, the number of received packets to be relayed etc.. The data is stored in secure files and completely managed by the program Avicoop.

This module also recognizes the statistical observations and decides the fate of the node. It is responsible for the detection and interception of any act likely to manipulate the system in place that can lead to the demand of the administration rights of host owner. Figure 1 below shows the functional architecture of Avicoop. It highlights the mechanisms of packet processing, storage and the principle of operation as described above. This diagram shows the operation of the Avicoop module in form of layered model. Layer (1) represents the Avicoop application embedded on each node by the layer (3) via an interface layer shown in (2).

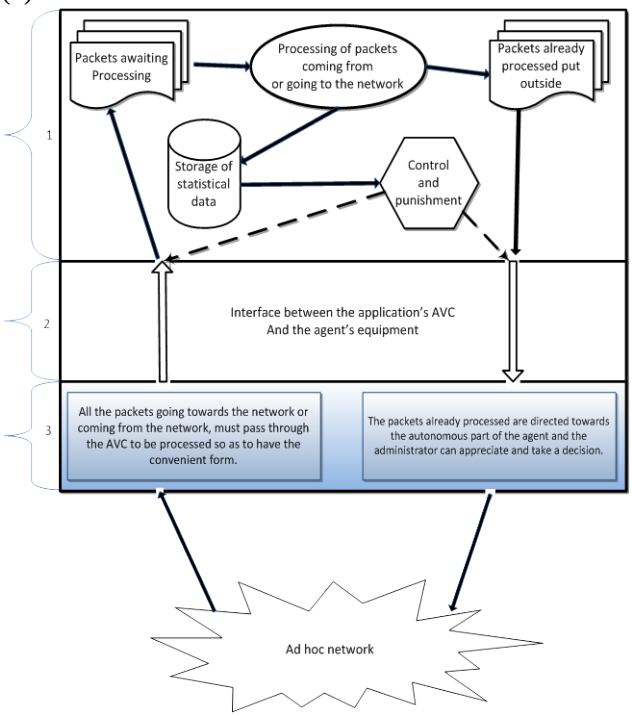

Fig. 1 Functional architecture in layer Avicoop

4. Computer Simulation of Avicoop Model: analysis and implementation.

The parameters of our system makes it closer to the field of multiagent systems [12], [13], we built our model according to the standard of this field [13]. It is implemented by agents.

4.1 The module behavior.

To simulate the behavior of the user of the equipment, we will provide each node of a module behavior, responsible

for the role of the node manager: receiving, sending, and destroying packets.

4.2 The processing module.

Note that depending on the sensitivity level of service to control, one can decide whether to toughen the punishment administered to nodes that refuse to cooperate in the process put in place. In our case, we will have more counters then analyzed values will enable us to make the final decision.

i) **A counter for messages destined for node:** this counter is initialized to zero and is incremented each time an incoming packet carries the address of the node.

ii) **A counter for packets received by the node to query the service relay**: this counter is also initialized to zero and is incremented each time the node receives a packet that it is not intended for it.

iii) **A counter for relayed packets (RP):** here, the sender is not the node; this counter is initialized to zero and is incremented each time the node relays a packet.

iv) **A counter for sent packets (SP):** here, the sender is the node itself; this counter, initialized to zero, is incremented each time the node sends a packet.

v) **A counter for bad packets:** this counter is initialized to zero and is incremented when the node sends a message like: unknown location and unknown road.

4.3 Calculation of reputation and punishment.

In our approach, we only focus on the parameter ***number of not relayed packets by a node***. We set:

- ***N0***: The number of not relayed packets.
- ***N1***: The number of packets received by the node to be relayed.
- ***N2***: The number of packets actually relayed by the node.
- ***N3***: The number advertising the non-compliance of messages
- So, N0 = N1 - (N2 + N3)

Remarks

- ***RP***: relayed packets
- ***PTR***: Packets to relay = received packets - Packets for the node
- ***NRP***: Not Relayed Packets = TPR-RP

When N0 is larger than a fixed Nmax1, the module of punishment passes only two out of three packets that take the original node. When N0 is greater than a fixed Nmax2, one passes a packet of two, and when N0 is larger than a fixed Nmax3, the node cannot transmit through the network. When N0 is larger than a fixed Nmax4, the node is automatically removed from the network. In the latter case, the node is relegated to an area of rehabilitation. It is a set of nodes to which we entrust the less sensitive network tasks to test their conversion. A test of re-integration will be made on such nodes before they even engage in the tasks of cooperation.

For the need of building our simulation platform, the analysis of the problem led us to model agents as classes of agents. We have identified five numbered from 0 to 4 we present below:

- **Class 0 agents**: these are agents that want to enter the network.
- **Class 1 agents**: these are agents that always obey the rules set. They fully cooperate in the mechanism of operation of the network adopted.
- **Class 2 agents**: these are agents that start by cooperating and end up by sulking the cooperation.
- **Class 3 agents**: these are agents that only become operative only when the control program adopts punitive measures and constraints.
- **Class 4 agents**: they do not cooperate in the routing mechanism established for the operation of the network.

Figure 2 shows the traffic between agents and describes the protocol of data exchanged over the network. Two devices belonging to a MANET send each messages of type **propagate** that are messages containing information for a network node. Messages of type **inform** or **acknowledgements** are messages that the module Avicoop of and node sent directly to that of another node to transmit information on the messages routing. Messages of type **request** are those sent by a node to request to join the network. The answer is a message of type **accept-proposal** that indicates whether the new node must belong to the network or not. Messages of type **confirm** (respectively **refuse**) are those Avicoop sends to the node to confirm its authorization to issue a message if the node has a good reputation (respectively to deny that the node sends a message if it is sanctioned by Avicoop). Messages of type **propose** are those that Avicoop sends to the node offering it to relay a packet. Messages of type **agree** are those addressed to the node.

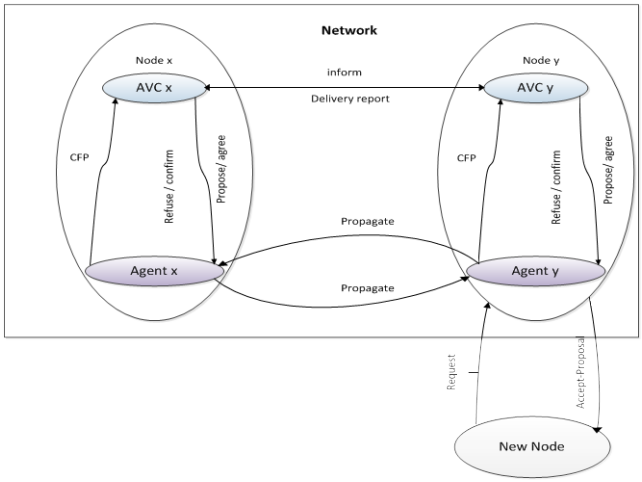

Fig. 2 Protocol of data exchanged

4.4 The different diagrams of the system

Figure 3 shows the system use case diagram. That of Figure 4 shows its state diagram.

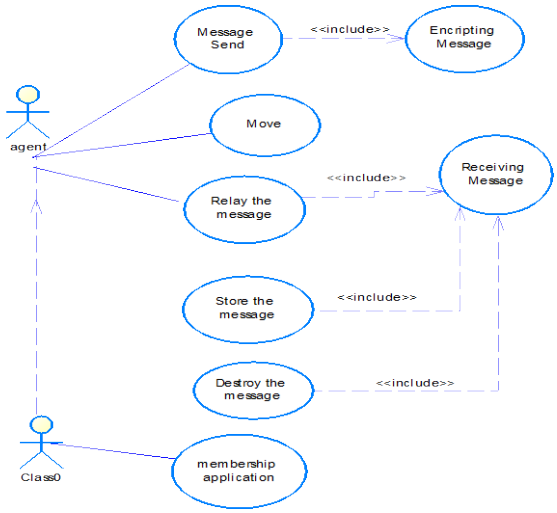

Fig. 3 System use case diagram

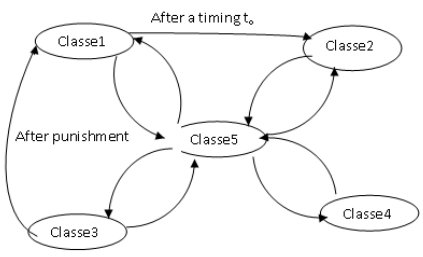

Fig. 4 System state diagram

Figures 5, 6 and 7, respectively present the sequence diagram and illustrate the dynamics of the system. The first (Figure 5) shows the inclusion of a configuration request by an agent entering the network. It presents the situation of a new node seeking to join the network. It must do the following operation:

- Identify proximity nodes that are already in the network
- Send a request for membership to the nearest host. If it does not respond after a delay time to; send another request to other host and so on.
- At the first positive response, send an acknowledgment to the sender.

Validate the Avicoop program and become a member of the network.

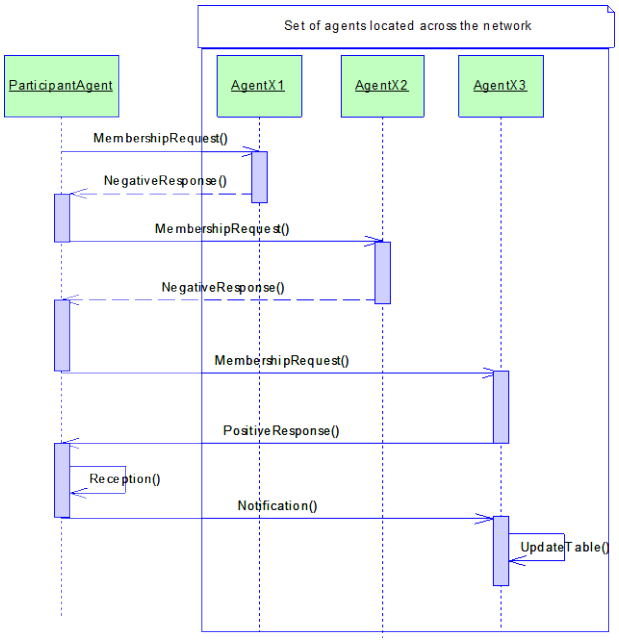

Fig. 5 Request for configuration by an agent entering the MANET

Figure 6 shows the sequence of messages exchanged between agents and Figure 7 shows the reception and relay of messages by a cooperating agent. Figure 8 shows the class diagram at the base of the implemented prototype.

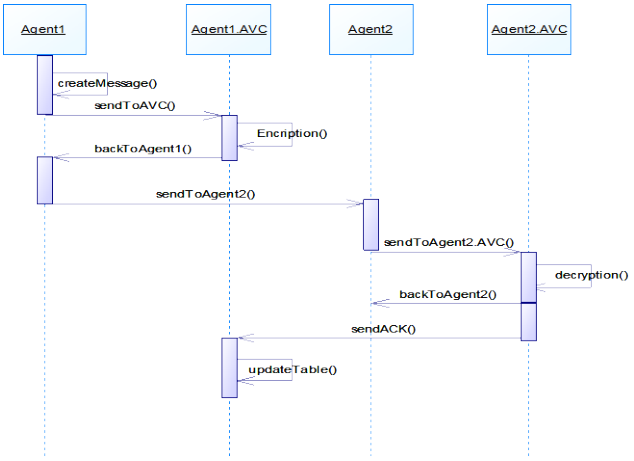

Fig. 6 Exchange of messages between two agents

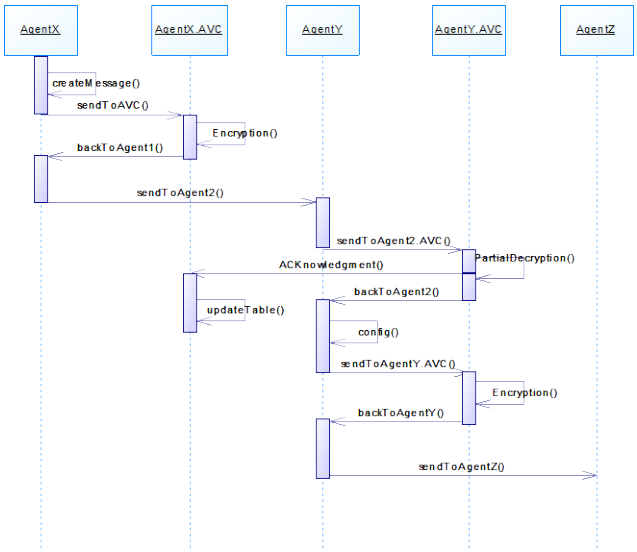

Fig. 7 Sequence diagram of message receipt and relay by a cooperating agent

4.5. Avicoop Simulator

The prototype was built in Java using Netbeans IDE 6.7.1 and JADE[1] agent platform 3.6. The software-jmf 2_1_1e-windows-i586 and the library jgrapht-0.8.1 were also required. At the start of the simulation, one must specify the number of agents per class (see section IV-C) as shown in Figure 8 and click on the button "**simulate**" to start simulation. A default delay of 50 seconds allows observing the movement of agents and their behavior on scene.

Fig. 8 Sending of a message by a Class 3 agent

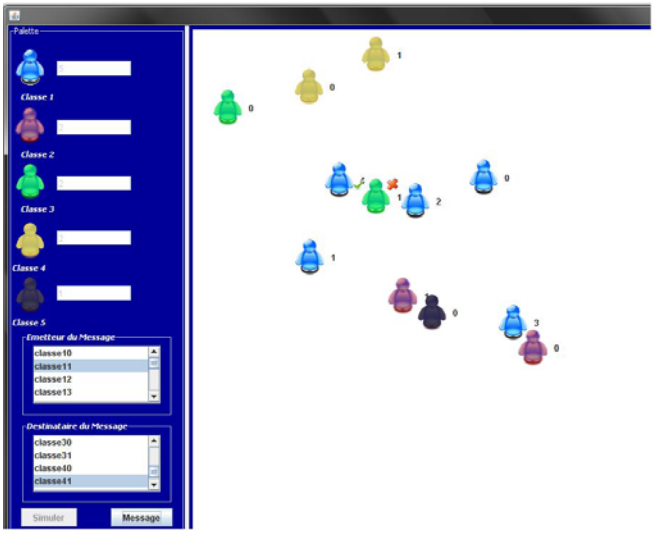

Fig. 9 Destruction of a message by a Class 2 agent

When an agent wants to send a message through the network, it scans its coverage area, as shown in Figure 8 by a concentric radiation. It calculates and transmits the message to the recipient if possible or to an agent in its vicinity to relay it otherwise. The intermediate agent destroys the packet if it is malicious and a cross appears to signify it on the simulation interface (Figure 9). The statistics are obtained for each agent at any time by simply placing the mouse cursor on the agent in question through the tooltip seen. A view to improve the simulator is to materialize the behavior change of agents. For example, an agent which does not cooperate should change color if it changes behavior.

[1] http://jade.tilab.com/, March 2012

5. Validation by the game theory

Our validation approach inspires from the Pietro Michiardi's works [11] thus researches on the cooperation in ad hoc field led to a model called CORE which, just like Avicoop, place each network node in a similar situation with that of the players of a game called dilemma of the prisoner that we present more in detail hereafter.

5.1. Brief overview on the concept of the game theory

1) Definition, presentation and typology.

The game theory is concerned with problems of strategic interaction of rational agents pursuing their own goals. It is interested in situations where involvers still called players or agents, make decisions, each one being conscious that its profits depend not only on its own decision, but also of the decisions taken by the others [14], [15], [16], [17], [18], [18]. A strategic game [19] is characterized by a set of game rules specifying:

- **Players:** it is a set of agents (physical persons, companies, countries, …)
- **Strategy spaces**: set of actions or decisions that are provided to players.
- **The sequence of decisions**: characterizes the running of the game. When players simultaneously decide, one speaks about game with simultaneous decisions in the contrary case, one says that the play is with sequential decisions. If in a game, each player only decides once a time, one says that the game is static. A repeated game is the reproduction of a static game called basic play. A repeated game is at finished horizon if the number of reproduction of the basic game is finished, in the contrary case, the repeated game is known as at infinite horizon.
- **Gains or the utility of players** (depending on of the decisions of players): they are players' payments according to the collective decision which conditions the game result.
- **The information available to the players** (complete / perfect). We have several games typologies: with simultaneous or sequential decisions, static or repeated (in finite or infinite horizon), with perfect or imperfect information, and games with complete or incomplete information. The game is known as with perfect information [19] when each player knows exactly his position (i.e the way or the history of the game) at the time to make any decision. One speaks of complete information [20], [21] when the functions about payment are known of all.

We recall here some other important definitions. **A strategy in game theory** is a comprehensive action plan specifying what the player will do at every stage of decision and deal with each situation that may arise during the game [10]. The **concept of strong assumption on the rationality of players** is based on the notions of **perfect rationality** and of **common knowledge of the game**. The perfect rationality refers to the ability to understand the game, computing and inductive backward reasoning. The common knowledge of the game is expressed as follows: I understand the game, and I know the others also understand the game and I know they know I understand the game and I know they know I know they also understand the game, etc [19], [20]. There is also a concept of representation of the game: the **how to represent a game**? Two approaches are available [14], [15], [16]: as a tree or extensive, tailored approach to games with sequential decisions and in normal or matrix form, it is suitable for (static) games with simultaneous decisions.

2) Concepts of game solution [14], [20], [21].

A solution is a description of strategies which would be adopted (and thus results obtained) by "normal" individuals in the context of interactions.

- **Concept of dominant strategy** [14], [15], [16]. A dominant strategy is defined as a strategy bringing the highest gain vis-a-vis all possible strategies of other players. When a state corresponds to a dominant strategy for each player, it is an equilibrium state in the sense that if all the players agree to adopt it, then the agreement will be respected by of all.
- **Concept of Nash equilibrium** [17], [20], [21]. A Nash equilibrium is a state in which no player whishes to change its strategy being given strategies adopted by other players. Each strategy is a better response to the strategies of other players. The Nash equilibrium is a situation likely or expected when players interact strategically.
- **Concept of correlated equilibrium** [18], [19], [20]. The concept of correlated equilibrium is an equilibrium lower than the Nash equilibrium with the role of a mediator in the presence of multiple equilibria or equilibria in mixed strategy.

In the rest of the paper, we are only interested in the concept of Nash equilibrium.

3) Concepts of commitment and credibility [14].

A **Commitment** is an engagement on a decision or a further action in response to decisions of other players. There are two types of commitment: (1) ***threats*** (punishing those who would not play the expected action) and (2)

promises (reward those who would play the expected action). A **credible commitment** (in the eyes of other players) is only made if the author has interest to do so in due course. Incredible commitment is worthless for others.

5.2. Model of the system

Avicoop exploits the game theory coupled with the Tucker model still called the prisoner dilemma. Here we quickly present this model.

1) The prisoner's dilemma (PD)[20], [21], [22], [23].

The dilemma of the prisoner is a famous example of the game theory represented by two people arrested together in possession of weapons and both suspected of a common offence. The police force, not having sufficient pieces of evidence to obtain the judgment of the defendants for the act of which they are accused, the consent of at least one of both is thus essential. The police officers separate them and explain the situation to each one:

- If one of both acknowledges (one says that he denounces his partner: D) and that the other does not acknowledge anything (one says that he cooperates with his partner: C), the first is released, and the second is imprisoned (5 years of prison sorrow);
- If both acknowledge, both will go in prison (3 years);
- If none of both acknowledges, both will be released at the end of one year because there was possession of weapons.

The question is to know which choices will make the prisoners. The table 1 below shows the matrix canonical representation of the prisoner's dilemma.

Table 1: Matrix canonical representation of the Prisoner's Dilemma [24], [25]

		Player 1	
		C	***D***
Player 2	***C***	(-1,-1)	(0,-5)
	D	(-5, 0)	(-3,-3)

One speaks about dilemma because this game emphasizes a disagreement between the individual interest (D, D) and the collective interest (C, C). The search for the Nash equilibrium (solution of the game) leads us to the situation where each player decides to acknowledge or to denounce the other (D, D). Indeed, if one puts oneself at the place of prisoner 2, if he acknowledges, whatever the strategy of the other, it will obtain a weaker custodial sentence (-3>-5 and 0>-1), consequently, player 2 does not may find it beneficial to play another thing than only acknowledge. The game being symmetrical on the profits level, one obtains in a dual way the same result for the player 1. However, one observes in the matrix that there exists an exit more favorable to both: (- 1, -1) related to the strategies (C, C). How then, the two prisoners could manage to make this choice whereas their strategic choices lead them to (D, D)?

The generalization [8] of this traditional model of the PD represents the situation of two players who must make the decision to cooperate (C) or not to cooperate (one speaks to denounce: D). This decision is made in a synchronous way, without a priori and without knowing the choice of the other. If the two players cooperate they receive a payment (R). If the two players decide not to cooperate they receive a payment (P). In the case where only one player cooperates while the other does not cooperate, the payments will be (T) for the player who did not cooperate and of (S) for the player who cooperated; the constraint being: T> R> P> S.

Table 2: Generalized matrix canonical form of the prisoner's dilemma [11]

		Player j	
		C	***D***
Player i	***C***	(R, R)	(S, T)
	D	(T, S)	(P, P)

The PD received much attention in the past thanks to the full applications' possibilities which recover fields such as the cooperation evolution study the in biology. Precisely, the PD belongs to the class of games named games with two players, whose sum of profits is not null, with a selection of simultaneous strategy.

A MANET composed of N nodes can be seen as a community (association, cooperative) of N individuals which interacts and whose existence depends on the participation (respect of the cooperation contract) of all and of each one. In the traditional operation of the ad hoc networks, each individual (node) must decide to respect or not the cooperation contract. One can establish an analogy with the dilemma of prisoner by considering a game which opposes each individual (node) to the community represented by a cooperation contract. The cooperation contract is replaced by Avicoop which represents the sovereign interest of the network. This being:

- to cooperate means to respect the cooperation contract i.e the protocol defined by Avicoop: one has the right to receive a payment R if Avicoop cooperates (i.e Avicoop allows the node to profit from network services) and S if not;

- the strategy of non cooperation for a node, it is to unilaterally refuse to respect cooperation clauses i.e non respect of the protocol defined by Avicoop: individuals with right to a payment T if Avicoop cooperates or P if not.

To validate our PD-based approach, we must justify the relation which characterizes it: T> R> P> S.

- the node gains S when it takes part in the good performance of the network (cooperates) and that in return, the community (Avicoop) does not render back the service (does not cooperate). It is clear that S is the lowest possible payment (thus T, R, P are all larger than S).
- the node gains R when he cooperates and that in return, the community renders back the service. In this case, it spends a little for the operation of the network but in return, it is assisted contrary with the situation where it does not cooperate and it does not profit from any assistance for a payment P. One then has R> P;
- finally, the highest payment (T) occurs when the node does not cooperate and that community continuous to render service to him. There is consequently T> R.

In the final analysis, one showed on the basis of realities of the ad hoc network that T> R> P> S, which allows us to affirm that the interaction between nodes of an ad hoc network and the selection process of the level of cooperation can be described by using a PD's model.

The only generalized Nash equilibrium of the PD is the strategy of non cooperation (D, D). It is simple to see that, while supposing fixe the choice of its adversary, the best a player can make to avoid losing (i.e. not to pay) is to choose the strategy D. the way in which the players choose their strategy is dictated by the principle of rationality: not only players are egoistic, in direction that they want to maximize their profits, but they have at disposal a computing power enabling them to guess the strategic choice of the adversary.

Our interpretation is as followed. A node's behavior is dictated by the rationality concept and the profit research which is part of an ad hoc network will choose not to cooperate in the process of packets routing. The theory shows that in an environment where each one seeks its profit in rationality, the single best alternative to make is that one. Let us note that this result is only valid if we consider that the game is only played once. That implies the absence of punishment on behalf of the competitors here represented by Avicoop. Consequently, it becomes necessary to set up a mechanism which will oblige players the cooperation.

2) Iterated version of the prisoner's dilemma [20].

The static model presented in the above section can be enriched by considering a game which consists in repeating a certain number of times the same game. In the scenario we consider in this paper, the interaction between a node and the network is often extended to more than only one exchange. In this context, the strategy chosen by a player in the past must have an influence on the future decision of its adversary. The remainder of the network is represented here by the Avicoop application. The influence concept evoked above references the calculation of the node reputation and punishment in the event of bad reputation.

Like the theory shows, it is possible to observe the evolution and the birth of the cooperation even if the basic game indicates that the only possible result is the non-cooperation, and especially even if players are guided by selfishness. It should be noted that in this section one considers the game repeated an infinite number of times. A principle known under the name of "inverse induction principle" [11], shows that the simple fact of knowing with certainty the end of the repeated game induces a non-cooperative behavior. Players, on the basis of the game last stage can apply the principle of rationality and not cooperate to obtain a profit at the time of, last iteration.
The inverse induction principle can be applied on the iteration before the last one of the game backward until to the first meeting, compromising a positive result which goes in the direction of the birth of a cooperative behavior. In practice, our model is based on a nuance of the concept of the indefinitely repeated game (often named game with infinite horizon) [11]: instead of repeating the game an infinite number of times, players do not quite simply know the end of the game. In this context, the shade of the future has a determining weight for game evolution towards a cooperative behavior. To conclude this short introduction to repeated games, it is necessary to characterize the utility function [25] maximized by players:

$$U_i = \sum_{t=0}^{\infty} \delta^t u_i^t \text{ ,[11]}$$

Next, one will thus consider the player *i* which maximizes the U_i function; this function being the sum of the utility function u_i of each iteration of the PD's basic game. The U_i function represents for example the interest that the node extracts from the network at the moment *t* of the interaction execution. The factor δ^t indicates the weight of an immediate profit compared to a long-term profit.

Axelrod in [20] use a tournament simulated on computer to numerically detect the strategies which could lead to the birth of the cooperation between players involved in a

iterated PD. In their experiment, 14 complex strategies and a completely random strategy are in competition as of the first iteration for a succession of 200 iterations. The unexpected result of this experiment is that a very simple strategy has proven to be the one that allows players who adopt it to gain the maximum of profits. This strategy is named the strategy tit-for-tat (TFT): to cooperate as of the first iteration, then to copy the adversary strategy used in the preceding iteration.

The adaptation which we make in the case of Avicoop is the following. The ad hoc network is defined as being a mesh network consisted of a collection of wireless and mobiles nodes without the assistance of a pre-established infrastructure used to carry out basic network management functions like the packets routing and forwarding. Our modeling led us to consider a game at the level of each equipment which puts the equipment in interaction with the rest of network through the Avicoop module. Avicoop represents the interest of the community vis-a-vis that of each equipment. The specification of stakes shows us that we can adapt this situation to a game already formalized and very studied known as dilemma of the prisoners. It introduces results which we try to exploit in our work.

The decision to collaborate or not in a network management function depends almost on the will of the user of the equipment in question. Thus, we can say that each node is rational in the sense that its user is. We suppose that a node is regarded as having deviated of the cooperation when it destroyed a number of network packets considered to be inconceivable as described in the Avicoop design solution. The Avicoop application always starts by allowing each node to be able to convey its packets through the network (one can thus say that Avicoop starts by cooperating) then, when a node deviates of the cooperation, Avicoop also begins by not collaborating any more (Avicoop copies the behavior of the node through its agents). It results from this that Avicoop adopts the behavior prescribed by the result noted above. One then concludes that Avicoop and consequently the network will benefit from the game.

6. Conclusion and perspectives

We were interested in a question which arises in the literature [1], [2], [3], [4] concerning the set of routing protocols in the ad hoc networks. Indeed, in their operation, each one of these protocols counts on the cooperation of each node by completely being unaware of the autonomous character of node which of this fact can accept, refuse or handle the principle of the protocol. The Avicoop approach draws inspiration from literature to develop a solution which introduces the following positive points:

- **The quasi-total decentralization of its implementation**: contrary to other solutions which recommend the presence of a certification authority, Avicoop approach does not centralize anything. Its implementation, its operation and its distribution are done at the level of each terminal. That undoubtedly increases the complexity level of its design because such a solution must as much as possible get closer to perfection. As no computing system is reliable at 100%, this opens on a concern that we did not address in this paper (perspective 1).
- **The application's autonomy**: the Avicoop application, based on the MAS is completely autonomous. The user of the equipment does not have the possibility of impacting on the application configuration in its favour. Thus, the application installation must register in the system of each equipment, indices relating to its passage in the network and its reputation. These indices are recognizable in the event of return of the equipment in the network (after for example an exclusion).
- **Security**: our security model is original in the context of MANETs, in this that it integrates an intelligent encoding and decoding module. Thus, one will no more have to flood the network with packets to share the coding keys as other solutions propose for solving security issues.

In term of perspectives, we project (1) the development of mobile agents for the configuration, update and maintenance of programs (Avicoop) through equipments of the ad hoc network. We question to how one could apply Avicoop in the fields of teaching and medical diagnosis. In the teaching, it would help for example a teacher to distribute a course document which can be automatically transmitted from one student to another on a MANET Campus. It can be necessary to know students who do not cooperate in this process. In the case of the medical diagnosis, a doctor could exploit Avicoop to collect medical information on its patients or to give information to them on an ad hoc network in a hospital environment. The doctor can need to support of this application to reflect or relay information. It also can be very useful in the epidemiology survey.

References

[1] Q. Le-Trung, G.Kotsis "A Network Model for MANET Nodes and Actors Collaboration to Optimize Processing in Event Areas" in Proc. PE-WASUN'07, ACM 2007.

[2] C. Chaudet, I.G. Lassous "Quality of Service in Mobile Ad hoc Network (from the originale title Qualité de service dans les réseaux mobiles ad hoc), in Proc. CFIP'2006, 2006.
[3] D.B. Johnson, D.A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", in Proc. of Mobile Computing, Imielinski, Korth, Eds, 1996.
[4] C. Perkins, E. Belding-Royer, S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. Request for Comments: 3561, July 2003.
[5] Nadjib BADACHE, Présenté par Tayeb LEMLOUMA - Le Routage dans les Réseaux Mobiles Ad Hoc.
[6] Marti, T. Giuli, K. et M. Baker, « Mitingating routing misbehavior in mobile ad hoc networks », Proceeding of The sixth International Conference on Mobile Computing and Networking.
[7] Seila Nuon, - Analyse de la disponibilité dans les réseaux Ad hoc - Etude bibliographique, 1 février 2006.
[8] ANDRIAMADY – Miarisoa Faniry, Tarification et réseau ad hoc, étude bibliographique - DEA en informatique.
[9] L. Buttyan and J-P. Hubaux, Switzerland Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks - Laboratory for Computer Communications and Applications Swiss Federal Institute of Technology – Lausanne EPFL-IC-LCA, CH-1015 Lausanne.
[10] A. Beghriche and A. Bilami- "Modélisation et Gestion de la Confiance dans les Réseaux Mobiles Ad hoc". Département d'informatique, Université de Batna–Algérie. 05,.
[11] P. Michiardi, "Coopération dans les réseaux ad hoc : Application de la théorie des jeux et de l'évolution dans le cadre d'observabilité imparfaite". In Proc. SSTIC06, 2006.
[12] C. Hütter, K. Böhm "Performance models for large scale multiagent systems: using distributed POMDP building blocks" in Proc AAMAS '03, 2003
[13] G. Picard, "Méthodologie de développement de systèmes Multi-Agents adaptatifs et conception de logiciels à fonctionnalité émergente.", PhD Thesis, University Paul Sabatier of Toulouse III, 2004.
[14] E. Altman, T. Basar, T. Jimenez and Nahum Shimkin, "Routing into two parallel links: Game-Theoretic Distributed Algorithms", Special Issue of Journal of Parallel and Distributed Computing on "Routing in Computer and Communication Networks", pp. 1367-1381, Vol. 61, No. 9, September 1, 2001.
[15] E. Altman, T. Basar, T. Jimenez and N. Shimkin, "Competitive routing in networks with polynomial cost" , IEEE Trans. on Automatic Control, Vol 47, pp. 92-96, Jan. 2002.
[16] E. Altman and H. Kameda, "Equilibria for multiclass routing in multi-agent networks", in Advances in Dynamic Games, Vol. 7, pp. 343-368, 2005
[17] E. Altman, T. Basar and R. Srikant , "Nash Equilibria for Combined Flow Control and Routing in Networks: Asymptotic Behavior for a Large Number of Users" in IEEE Transactions on Automatic Control, Special issue on control issues in telecommunication networks, Vol 47 No 6, pp. 917-930, 2002.
[18] E. Altman , A. Silva , P. Bernhard , M. Debbah, "Continuum Equilibria for Routing in Dense Ad-hoc Networks" in Proc. of Forty-Fifth Annual Allerton Conference on Communication, Control, and Computing, PP 26-28, 2007.
[19] T. L. Turocy, B. von Stengel, "Game Theory", CDAM Research Report, an introductory survey of game theory, In Encyclopedia of Information Systems, Academic Press, 2002
[20] R. Axelrod, "The Evolution of Cooperation", Basic Books, 1984.
[21] Roger B. Myerson, "Game Theory: Analysis of Conflict" 2007
[22] wikipédia, "Prisonner's dilemma", (http://en.wikipedia.org/wiki/Prisoner's_dilemma
[23] J. Li, G. Kendall, "A strategy with novel evolutionary features for the iterated prisoner's dilemma" in Evolutionary Computation, Vol 17 Issue 2, MIT Press, 2009
[24] S. Lemp "Sciences et Technologies de l'Information et des Matériaux- Médiation flexible dans un système pair à pair". PhD Thesis, Université of Nantes- STIM Doctoral School, 2007;
[25] B. Beaufils, "Intelligence artificielle & intelligence collective - Théorie des jeux" ; Course material avaliable online at www2.lifl.fr/~beaufils/mri/theorie_des_jeux.bruno.pdf, 2007 (acceessed March 2012.

Thomas Djotio Ndié, PhD, Engineer is a post graduate Computer Science Engineer since 1997 and PhD since 2008 from the Ecole Nationale Supérieure Polytechnique (ENSP) of the University of Yaounde 1 – Cameroon. He has been working as software developer, system and network administrator, entrepreneur, author and trainer. Thomas is a MCP, CCNA and Security + Certified. His research areas are intelligent systems for network administration and security, threats investigation and mitigation, network and telecommunication protocol definition. He is currently the MASECNeSS' Scientific Team Leader of LIRIMA (http://www.lirima.org) and senior Lecturer at the National Advanced School of Engineering (ENSP) teaching information and network security, operating system, network technology and administration and system programming.

Claude Tangha, Dr, Professor has been teaching since 1976 at the Ecole Nationale Supérieure Polytechnique (ENSP). His research areas are software engineering, e-learning and artificial intelligence including expert systems, multiagent systems, and formal systems. He has directed many research projects, contributed to many conferences and seminars nationwide and at the international level. His personal website is http://www.mbounde.org/. He is currently the Chief of the Department of the Computer Engineering at the ENSP of the University of Yaounde 1 – Cameroon and the Director of the Laboratoire d'Informatique, de Méthodes et Modélisation des Systèmes (LIMMS, ex-LABORIMA) and ALOCO Scientific Team-Project Leader of LIRIMA.